AMENDMENTS TO THE SPECIFICATION

I. Please amend paragraph 0026 on page 6 of the Specification as follows:

A variant of the method is to assign a special role to one of subscribers T1-Tn for the execution of the second method step. If this role is assigned, for example, to subscriber T1, then method steps 2 and 3 are executed only by subscriber T1. In fourth method step , all subscribers T1-Tn involved in the method compute common key k according to the assignment k: = h(z1, g^{z2}, ..., g^{zn}), it being required for h(x1, x2, ..., xn) to be a function which is symmetrical in arguments x2, ... xn. This variant drastically reduces the number of messages to be sent. An example of such a function [[g]] h is, for instance,

$$k: = h(z1, g^{z2}, ..., g^{zn}) = g^{z1 \cdot z1} \cdot g^{z2 \cdot z1} \ ... \ g^{zn \cdot z1}.$$